[0024] to suppress generation of charging data record (CDR), particularly suppression of those CDR's in lawful interception scenarios for a monitoring call leg, insofar as at least partially a generation of data records is suppressed in the sense that sensitive information is not contained; and

[0025] an extra benefit may reside in the fact that the transit-MSS can also hide/suppress statistical reports about the monitoring calls (as in statistics, basically the same problem exists like in charging: sensitive information might appear in the statistical reports, unless these informations are suppressed/removed).

BRIEF DESCRIPTION OF DRAWINGS

[0026] For a more complete understanding of example embodiments of the present invention, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

[0027] FIG. **1** illustrates an example of a usable message data format according to the referenced ETSI standard;

[0028] FIG. **2** illustrates an example scenario in which a calling party is intercepted or monitored;

[0029] FIG. **3** illustrates another example scenario in which a called party is intercepted or monitored;

[0030] FIG. **4** illustrates a basic block circuit diagram of a network entity such as a MSS or also a transit MSS in which embodiments of the present invention are implemented;

[0031] FIG. **5** illustrates an example of a processing flowchart for a network entity such as a MSS; and

[0032] FIG. **6** illustrates an example of a processing flowchart for a network entity such as a transit MSS.

DESCRIPTION OF EXEMPLARY EMBODIMENTS

[0033] Example aspects of the invention will be described herein below.

[0034] In brief, according to one example or embodiment, in the above referenced ETSI standard, to which reference is made as a mere example only, there is the so called correlation information, which is sent in the Calling and Called Party Subaddress field in an initial address message, i.e. the IAM. In the Called Party Subaddress, one of the fields is the Operator ID (Octets 4, 5, 6), which is a configurable parameter in the MSS (See ES 201671 V3.1.1, annex E.3.2, Field order and layout). Since this subaddress is needed for the monitoring centre (authority equipment), this field propagates through all the MSSs. Hence, also in the Transit MSS it can be checked the Called Party Subaddress of the IAM whether it contains the predefined Operator ID, and (at least optionally) whether this is in the right place, and if those match with each other, then the PSTN call leg (monitoring call leg) is found to be a monitoring call. If this is detected, then the CDR generation is suppressed for this monitoring call leg. In Transit MSS, it is detectable whether the call is a monitoring call leg or not and if yes, then all the CDRs can be suppressed for that call leg. In this way, an operator will not know whether there is ongoing lawful interception in his network.

[0035] Generally, the invention is implemented in a mobile communication network.

[0036] FIGS. **2** and **3** illustrate example scenarios concerning interception or monitoring of either a calling party (FIG. **2**) or a called party (FIG. **3**). Firstly, in order to enhance understanding of the illustrated scenarios, devices/entities involved will be described. As shown in both Figures, FIG. **2** and FIG. **3**, a terminal A-party denoted by numeral **1***a* communicates with another terminal B-party denoted with numeral **1***b*. This communication is accomplished via the intermediary of an MSC server MSS-A denoted by numeral **2***a* and a further MSC server MSS-B denoted by numeral **2***b*. A respective terminal **1***a*, **1***b* can be a mobile station MS or a user equipment UE, for example a mobile phone or a smartphone or a personal computer/laptop connected to the mobile communication network. When setting up communication between A-party and B-party, A-party sends in a first message a setup including at least the address of the called party CDP=B. This message is sent towards the MSS-A. The MSS-A then forwards a message including the calling party address CGP=A# and the called party address CDP=B#, and so on which is forwarded to MSS-B **2***b*. The MSS-B **2***b* forwards the setup message to the terminal **1***b* informing him of the calling party's address so that this setup message contains at least CGP=A#. The MSS-A generates MOC (Mobile Originated Call) CDRs and the MSS-B generates MTC (Mobile Terminated Call) CDRs. Further, in case the calling party A is to be monitored by lawful interception authorized by law enforcement authority, the MSS-A, responsive to the setup message received from A-party, sends an initial address message (message **2** in FIG. **2**) towards the monitoring center **3** which is associated and/or connected to the law enforcement authority **3***a*. The initial address message passes through at least one transit MSC server. A transit MSC server can, for example, be a gateway MSC server or other MSC server. It is also to be noted that depending on the access point of a calling or called party, any MSS can take the role of a transit MSS depending on certain circumstances. Thus, functionalities in relation to the present invention describe distinctively for MSS-A and MSS-B on one side and the transit MSS on the other side are of course present simultaneously in each MSS but activated depending on the specific role in specific circumstances of the irrespective MSS.

[0037] With reference to FIG. **2**, MSS-A represents a network entity equipped with an apparatus comprising a control unit (see FIG. **4** for other details). The control unit is thus configured to detect a trigger for lawful interception of the calling A-party and responsive thereto, to compose a setup message to setup monitoring connections towards another entity, i.e. the monitoring center **3**, and further to establish such monitoring connection towards said another entity. The control unit is further configured to compose the setup message in such a manner as to include a preconfigured identifier representative for lawful interception and to set a setup message. That is, the initial address message sent to the monitoring center contains, within the called party subaddress, an operator ID as a preconfigured identifier representative for lawful interception. Such operator ID is preconfigured in all the MSSs of the network of a given operator.

[0038] Hence, in such particular example, the control unit is also configured to include said preconfigured identifier in a specific message field within said message and further, at least optionally, to include said preconfigured identifier in a subfield identifying said another entity to which the monitoring connection is established (the called party in the initial address message **2** in FIG. **2** is directed to the monitoring center as a called party in this call leg). Also, the control unit is further configured to include said preconfigured identifier at a specific location within said subfield identifying said another identity. Namely, the identifier is the operator ID in